ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

ACCESS CONTROL BASED ARCHITECTURAL FRAMEWORK FOR IMPLEMENTATION OF SECURED TPM ON E-COMMERCE

Chinyere G. Kennedy[1], DongSub Cho[2], Funminiyi Olajide[1 2]*, Samuel N. John[1 2]**
[1]Dept. of Computer Science and Engineering, Ewha Womans University, Seoul, South Korea.
[2]Dept. of Electrical and Information Engineering & Dept. of Computer and Information Sciences, Covenant University, Ota, Ogun State, Nigeria.
Email: gkennedy@ewhain.net

Received on: 20.10.2016 *Accepted on: 25.11.2016*

Abstract

This work designs a Trusted Platform Module (TPM) specifically intended to defend system clients from e-commerce criminals. A Trusted Platform Module (TPM) is specifically intended to defend system clients from e-commerce criminals to improve data security and system safety in e-commerce. Many challenges still lie on the path to improving security capabilities for e-commerce. In addressing these problems, this paper developed a dual TPM architecture for protecting e-commerce application server and to enhance robustness, flexibility and good performance of the database. It identified the various threats, and thus advanced solution mechanism via the creation of a robust TPM that minimizes system vulnerabilities and redundancy of both frame and personal computers. Also, Experiment results for the dual TPM indicated significant improvement in capabilities such as: login, email, web access, and protection of client's data. TPM specifically intended to defend system clients from e-commerce criminals. In this research, revealed that the dual TPM architecture is very reliable and not susceptible to failure. The implementation of this technique reassures clients' privacy, information confidentiality, and high safety.

Keywords: Access control, Architecture, TPM, e-commerce, Trust Platform Module (TPM)

1. Introduction

Trusted Platform Module (TPM) gives a number of cryptographic capabilities which is able to protect system clients from both known and unknown threats to the clients' information. TPM can be found in the motherboard of a computer, though recently it can be found in other electronic devices that require Trusted Computing (TC). The specifications of TPM are generated from the Trusted Computing Group (TCG). TCG defines TPM as "a microcontroller that stores keys, passwords and generates digital certificates." It affirms the root of trust in the TC.

In recent time, electronics transaction is becoming more popular, and it uses both computer and server. Electronic commerce (e-commerce) can be defined as "any form of commerce in which the buyer of a product uses a computer to interact with the computer system of the seller of that product or service". In other words, e-commerce is a virtual market created by computer networks with the users of the Internet and mobile devices as its customers. E-commerce creates a platform for selling virtual items such as book, software, electronics, equipment, household items and a whole of others. E-commerce deals with a whole lot of issues which need security alertness. It deals with multiple currencies from different countries of the world, and accepts multiple payment types such as: credit card, debit card, etc.This paper identifies the attackers in e-commerce and proposes a better architectural platform to enhance the present architecture that will prevent the success of such attacks. The TPM architecture was introduced on the aspects of identification and access control respectively. Figure 1 is a simple TPM architecture;TPM has a random number generator, a RSA key-pair generator that has limited storage and a cryptographic co-processor with servers as the foundation of trust for the whole software processes and services on the original platform. Endorsement Key (EK) and Storage Root Key (SRK) are two important 2048 bit asymmetric key pairs stored in the TPM, used to identity TPM and protect users' data. There are two kinds of administrators' manager in TPM known as TPM owner and TPM operator. When the owner could not remember the authorization password or is not available to execute the TPM commands, the operator can execute TPM managing commands based on Physical Presence, which implies direct intervention by a third party – i.e. operator assisting via the TPM. We cannot over emphasis the need for securing a network. Currently the biggest challenge facing ecommerce is insecurity and redundancy. For instance banking industry with a lot of data to deal with needs a secured, reliable device to work with. However, reasoning about this e-commerce and challenges were most often overlooked in past. Fortunately, contemporary researchers have been ahead trying to rectify bothering issues pertaining to e-commerce and how best to protect their data from hacker.

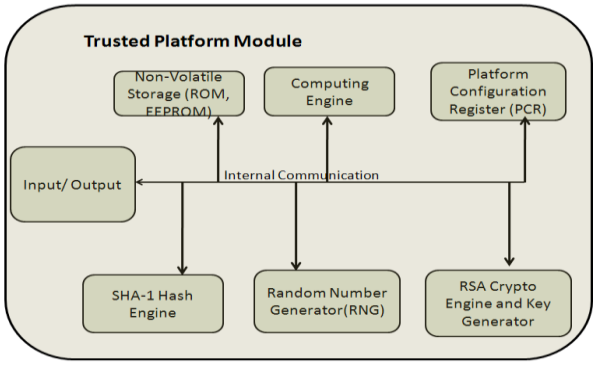

Figure 1.Simple TPM physical Architecture.

In order to avoid inefficiency in dealing on large communication with overlap contents in security measures: the authors have designed this device with dual TPM having the capability to establish a high availability. Relevant citations and critical examining of related work are included for background knowledge and to rationalize the technical significance of the current work. Description of the dual-TPM architectural framework and its advantages over extant designs are treated. The working principle of the dual TPM and its striking features are well elucidated. Suggestions for further research to enhance security for e-commerce are made.

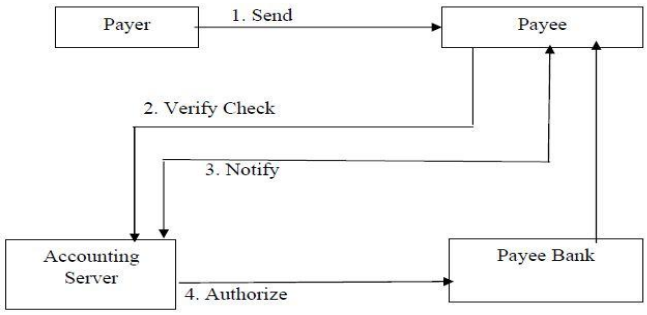

Figure 2.E-Commerce architecture[6].

A simple flow chart for electronic fund transfer is presented in Figure 2 above. Every fund paid to the receiver through the internet especially the bank, goes to the accounting server for verification in the bank computer, which authorizes the transfer. The system receives an instruction or authority to debit fund to the payer's account number. Our paper, however, creates a framework that enhances the authentication of this computer from which the fund will be transferred using TPM. When credit card or debit card are used some of the attackers that divert fund from the original owner to the hacker will be prevented by the TPM.

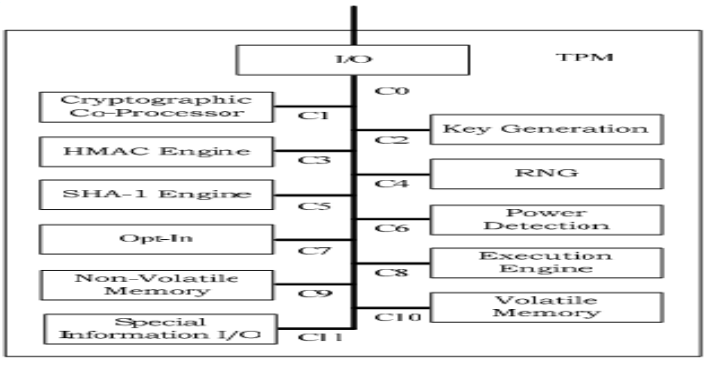

Figure 3.TPM Enhance Architecture.

Li et al in their paper "Enhanced Architecture of TPM" added a new special information I/O interface by connecting with various parallel or serial trusted devices outside. This new special information I/O interface replaced the function of the physical-presence and implementation of pre-configuration, backup, and the restoration of information within TPM. They considered the shortcoming of the TPM such as owner's unawareness; backup keys and restores keys

being captured by the Trojan horse or virus program, and lack of physical presence. With this technology TPM is not connected directly to the CPU instead it is connected to the physical presence such as USB port. Figure 3 shows how a TPM is built at the I/O device.

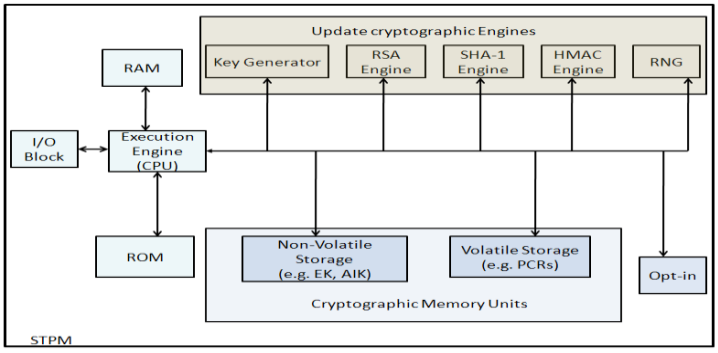

Figure 4.Sustainable TPM Architecture.

Malipatlolla et al showedin Figure 4 how a sustainable trusted platform module (STPM) can ensure a secure update of the TPM cryptographic engines without compromising the device's trustworthiness. STPM was implemented on Xilinx Virtex-5 FPGA platform, demonstration of a testing case with an update of the fundamental hash engine of the TPM was carried out. Updating a cryptographic algorithm on TPM technology needs a special architecture that can support secure update. Conventional TPM is in general an Application Specification Integrated Circuit (ASIC) which can be implemented but cannot be updated after deployment. STPM could dynamically load new cryptographic engines that are updatable. The most sensitive main information such as Endorsement key (EK), Storage Root Key (SRK) and Certification are stored in the non-volatile memory in a conventional TPM. Their STPM architecture has both static and dynamic regions, with volatile and non-volatile memory. STPM Update works by allowing the Computer system which has STPM embedded and the update server which maintains the library to be the main environment; it is used by dedicated staff.

Table-1.Resource Consumption of Static Logic of STPM.

	Reg.	LUT	36Kbit BRAM
AES-128	524	899	5
Hash-Core	289	138	0
HMAC-Core	294	184	0
Controller	662	453	0
PRICAP	170	168	7
Update Alogorithm	1939	1842	7
MicroBlaze CPU	2326	2704	4
Total Static Logic	4265	4546	11

The above Table 1 presents the summary of the overall resource consumption of the static logic implementation for both update algorithm and executed engine.

Update algorithm deals with the configuration of file for new hash engine while the executed engine control the flow and also commands of the TPM functionality.

A typical TPM device has these features as indicated in Figure 3. For instance, a nonvolatile storage which stores information in the memory of a computer when power goes off; a random number generator used to generate keys for various purposes; and a SHA-1 Engine for computing hash values of small pieces of data. Platform configuration Register guarantees registration to have a certificate. Key Generation enables the generation of keys such as Endorsement Key (EK), Attestation Identity Key (AIK) and other keys. The AIK provides platform authentication to a service provider and it does it anonymously. RSA Engine helps the platform to perform up to 2048bit on encryption and decryption. It is used during digital signing and key wrapping operation. Opt-in is built to make the user to accept "yes" before any particular function feature or service is provided. Program Code gives room for the software stack.

Computers infected by virus are effectively salvaged and secured by recent anti-viruses which study the behavior pattern of the virus and nullify its activities.

The virus warning center in China gave the Table2. The figure is still on the increase. This worrisome situation makes researchers to put more effort to see that the damage of virus is reduced. A researcher proposed secured device ID (identity)which will provide a unique identifier with a cryptographically bound to the device in order to use it to identify and authentic operations[1].This DevID can help to block viruses from have free access to computers or system devices[1].

Table-2.New virus and effected computers.

Year	*New Virus*	*Infected Computers*
2006	10375	18832094
2007	100017	34414776
2008	47743	27998478
2009	1015586	14933761
2010	91994	11533661
2011	66686	3743721

2. Our Proposed Architecture

With e-commerce so many new technologies are being introduced to meet up with the people's demand. This technology helps customers to access any product and service faster than in previous time. Instant conversion of currency, real-time trade, digital cash and smart card has been made possible due to e-commerce. E-commerce has a great future but there are many challenges that can affect growth of e-commerce such as: poor design of the platform, unhealthy competitors who can cause rival-systems' infection with viruses. Since e-commerce is internet based virus can be spread throughout a computer or network. Some viruses can delete files, lock file and slow down Personal computer (PC). The cluster virus is even a more dangerous virus for e-commerce because it has the ability to change an executable file to its code[2,3], thereby causing colossal loss of vital files. The underlying principle of our proposition is to identify the attacking virus and design an architectural framework that can provide a permanent solution. Our architecture will use authentication key to verify the ownership, and use same to give the owner the right to access the resource alone[4,5]. Then the encrypt key will make sure that during the communication or transaction the owner is not spied. The followings are the categories of Threats:

Spamming;

- Receipt of unsolicited commercial emails
- Receiving of bombing emails targeted to a computer or network
- Surfing which is about setting a third party system, , and sending message to intended target by using software
- Denial of Service Attacks: Hackers conquer the target by taking its resources

Viruses:

- Worms: It operates by using direct internet connections
- Trojan Horses: Pretends to be genuine software and allows the user to run it.

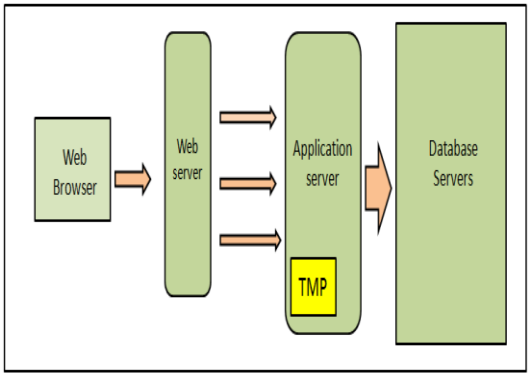

Figure 5. Architecture of TPM.

3. Our Approach

Our new approach involves the building of TPM architecture on an e-commerce application server to ensure high protection and enhanced performance of its database server. Usually, the breaking of security is the main target of the attackers as indicated in Figure 5. Also, the concept of this paper facilitates a stronger and a more dependable security on personal computer for e-commerce. Despite the enhanced security, the dual TPM has improved capabilities for: login, email, web access, and protection of data. Its architecture is very strong and robust to handle defects, even though failure is inevitable.

This method will enable the e-ecommerce system to avoid redundancy, and increase high availability in controlling associated technologies and systems' performances.

For the TPM to carry this out it needs store information specific for the host system such as encryption keys, digital certificates and passwords. The algorithm below shows TPM architectural simulation which displays the method that TPM uses to generate keys in dual TPM architecture.

Algorithm 1: Manager Controller Algorithm

```
Entity simulation is
  end simulation;
      architecture test1 of simulation is
      signal A,B: bit;
      begin
                  TPM1: Proceed(B)
                   Begin
                   A<= '1';
                   A<= transport '0' after 5 ns;
  end process TPM1;
  TPM2: process(A)
  Begin
  If A = '1' then B <=not B after 10ns; end if;
  end process TPM2;
end test1;
```

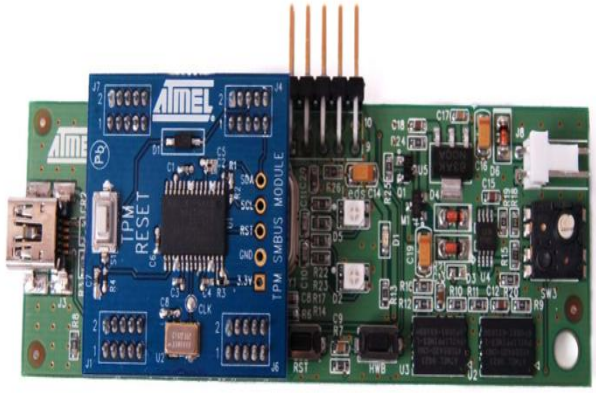

Figure 6. Embedded TPM mounted on AT90USBKey.

TPM deals with key management system. Figure 6 is an embedded TPM on AT90USBKey used during this experiment. XPort server is dedicated for the e-commerce. This experiment also has the capabilities of connecting devices through a TCP data channel or through a Telnet connection to computers or to another device server[6]. The XPort also supports UDP datagram which helps the device to relate with each other. It contains a web [HTTP] server that allows presentation of custom content and allows easy configuration through a browser. It uses three programmable I/O pins to monitor or control attached devices. The XPort device server can be applied in some[7] Ethernet networks using the IP protocol such as: ATM machines, CNC controllers, data collection devices, environmental sensors, Universal Power Supply (UPS) management units, telecommunications equipment, data display devices, security alarms and access control devices, handheld instruments, Modems, Timeattendance clocks and terminals.

This new approach has the tendency of having any computer device which has TPM especially (version 1.2) that provides a so-called hash value for the complete system by using SHA1 (Secure Hash Algorithm). This valued data is assembled from information gathered from all key hardware elements, such as the video card and processor, in combination with software elements (the operating system, among others). Some of the proliferation of mobile computing, electronic communication, and the sophistication of wired and wireless networks results in more complicated attacks and an increased vulnerability of the most important asset to an enterprise. There are always so many critical incidents that occur daily such as identity theft, information leakage, data destruction, sensitive data exposure due to lost or stolen notebook computers and unauthorized access to corporate networks. As consequence of this sensitive problem in many countries, government legislation is mandating increased security around valuable data in e-commerce sectors for specified vertical industries. With the increased vulnerability, businesses and consumers are also demanding a computing environment that is more trusted, private, safe and secure. It has the

capability to eliminate deceptive endpoint in Network Access Control (NAC) that is attached to the E-commerce server. The limitation of anti-virus software can be overcome by using the TPM with its hardware-based security, for integrity measurement and remote attestation [8-20].

4. Conclusions

Many challenges still lie on the path to improving security capabilities for e-commerce. In addressing these problems, this paper developed a dual TPM architecture for protecting e-commerce application server and to enhance robustness, flexibility and good performance of the database. It identified the various threats, and thus advanced solution mechanism via the creation of a robust TPM that minimizes system vulnerabilities and redundancy of both frame and personal computers. Also, Experiment results for the dual TPM indicated significant improvement in capabilities such as: login, email, web access, and protection of client's data. The dual TPM architecture is very reliable and not susceptible to failure. The implementation of this technique reassures clients' privacy, information confidentiality, and high safety.

References

1. Borza M, DevI D. Relationship to TPM. Elliptic Semiconductor. Proposed IEEE 802 Network.2004
2. Ishii H, Francis BA. Stabilizing a linear system by switching control with dwell time. IEEE Trans AutomControl, 2002, 47(12), 1962-1973
3. Lantronix Manual. http://ltxfaq.custhelp.com. 12/10/2014
4. Nabi F. Secure business application logic for ecommerce system. Computers & Security. 2005 May; 24(5),345-350
5. Sang SK, Yen YY, Sang HK, Seok KL. Research Direction of Constructive e-Business Consulting for SMEs and Medium-Sized Enterprises (SMEs). Focusing on e-Commerce Busines.Indian Journal of Science and Technology. 2015 April; 8(S7)306–313
6. Trusted computing for developer.http://www.trustedcomputinggroup.org. 16/07/2014
7. Syed TA, Musa S, Rahman A, Jan S. Towards Secure Instance Migration in the Cloud. Cloud Computing (ICCC), International Conference, 2015 April, 1-6
8. Li F, Wang W, Ma J, Ding Z. Enhanced Architecture of TPM. 9th International Conference for Young Computer Scientists:icycs, 2008,1532-1537.

9. Malipatlolla S, Shoufan A, Arul T, Huss SA. A novel architecture for a secure update of cryptographic engines on trusted platform module. Field-Programmable Technology (FPT) International Conference: 2011, 1-6.
10. Sailer R, Zhang X, Jaeger T,Doorn L. Design and Implementation of a TCG-based Integrity Measurement Architecture. 13thUsenix Security Symposium:San Diego, California, 2004.
11. E-Commerce and Security. http://www.it.uu.se/edu/course/homepage/ehandel/vt08: 06/03/2015
12. Goldman K, Perez R, Sailer R. Linking Remote Attestation to Secure Tunnel Endpoints. Conferece Computer and communications security. Proceedings of ACM STC '06, Virginia, USA, 2006,21-23.
13. Berger S, Caceres R, Goldman K, Perez R, Sailer R, Doorn L. vTPM – Virtualizing the Trusted Platform Module. 15thUsenix Security Symposium: Vancouver, Canada, 2006 July.
14. Camenisch J. Better Privacy for Trusted Computing Platforms. In proceedings of ESORICS. 2004, 73-88.
15. Bajikar S. Trusted Platform Module (TPM) based Security on Notebook PCs-White paper. Mobile Platforms Group Intel Corporation, 2002 June.
16. Das S, Wei Z, Yang L. Reconfigurable Dynamic Trusted Platform Module for control Flow Checking. IEEE Computer Society Annual Symposium, 2014166-171
17. Xport Manual. http://kc.koncon.nl/ipsonlab/downloads/xport_ug.pdf . 09/02/2015
18. Renesse RV, Birman K, Vogels W, Astrolabe:A Robust and Scalable Technology for Distributed System Monitoring, Management, and Data Mining. ACM Transactions on Computer Systems, 2003 May: 21(2) 164-206
19. WS_RELIABILITY, WS-Reliable Messaging, WS_Eventing. http://www.w3.org. 07/05/2014
20. Nichols JW. Using Handhelds as Controls for Everyday Appliances. A Paper Prototype Study, ACM CHI'2001 Student Posters: Seattle, WA,2001, 443-444.